Республиканский Кредитный Альянс

Коммерческий Банк

РЕКОМЕНДАЦИИ

о порядке действий Клиента в случае выявления или подозрения на хищение денежных средств с расчетного счета, обслуживающегося с использованием Системы дистанционного банковского обслуживания (ДБО)

В целях оперативной организации эффективного взаимодействия и принятия процессуальных решений по фактам совершения хищения денежных средств с расчетного счета Клиента при использовании Системы дистанционного банковского обслуживания (далее - ДБО) рекомендуем:

1. В случае выявления или подозрения на хищение денежных средств с расчетного счета, обслуживающегося с использованием Системы ДБО, немедленно прекратить любые действия с электронными устройствами (далее – ЭУ), которые используются для осуществления расчетов посредством ДБО, обесточить их (принудительно отключить электропитание в обход штатной процедуры завершения работы, извлечь все аккумуляторные батареи из ноутбука и т.п.) и отключить от информационных сетей (если было подключение, например, по Ethernet, USB, Wi-Fi, Dial-Up и др.) или перевести в режим гибернации ("спящий" режим). При отсутствии возможности обесточивания ЭУ, осуществить отключение по штатной процедуре и запротоколировать указанный факт.
2. При наличии технической возможности отозвать из банка распоряжение о перечислении денежных средств с использованием иного ЭУ, после чего принять меры к блокированию Системы ДБО.
3. При отсутствии технической возможности отозвать распоряжение о перечислении денежных средств с использованием Системы ДБО, немедленно обратиться в банк по телефону указанному в договоре, с заявлением о блокировке Системы ДБО, приостановке исполнения платежа и возврате денежных средств.
4. Произвести фотосъемку ЭУ (с подключенными кабелями и иными периферийными устройствами) рабочего места и его расположения в помещении. Обеспечить сохранность (целостность) ЭУ, как возможного средства совершения преступления, поместив его в место с ограниченным доступом, обеспечив при этом защиту от вскрытия (стикеры, наклейки, пластилин, мастичная печать, пломбы и т.п.) и по возможности зафиксировать средства контроля целостности фотографированием со всех ракурсов. Если позволяют размеры ЭУ, следует поместить его в непрозрачный пакет (мешок) и заклеить горловину.
5. Дополнительно к п. 2, п. 3 настоящих Рекомендаций, незамедлительно обратиться в банк с письменным заявлением об отзыве платежа, возврате средств, блокировании Секретных ключей и доступа к Системе ДБО (по форме Приложения № 1 к настоящим Рекомендациям), а также о компрометации Секретных ключей и необходимости смены пароля.
6. При наличии необходимой информации (реквизиты получателя) обратиться в банк получателя или к оператору соответствующей платежной системы с письменным заявлением о приостановлении платежа и возврате денежных средств (по форме Приложения № 2 к настоящим Рекомендациям).
7. Предпринять меры для обеспечения сохранности и неизменности записей с внутренних и

внешних камер систем видеонаблюдения, журналов систем контроля доступа, средств обеспечения и разграничения доступа в сеть Интернет (при наличии таковых) за максимальный период времени, как до, так и после даты совершения хищения денежных средств.

8. Провести сбор записей с межсетевых экранов и других средств защиты информации, серверов баз данных и иных компонентов клиентского приложения Системы ДБО, систем авторизации пользователей (AD, NDS и т.д.), коммуникационного оборудования (включая АТС), ЭУ, используемых для управления денежными средствами с использованием Системы ДБО банка, устройств, которые могут использоваться для удаленного управления указанными ЭУ.
9. При возможности оперативно обратиться с письменным заявлением к своему Интернет-провайдеру или оператору связи (по форме Приложения № 3 к настоящим Рекомендациям) для получения в электронной форме журналов соединений с Интернет, с ЭУ или из локальной вычислительной сети, как минимум за три месяца, предшествовавшие факту хищения денежных средств.
10. Не предпринимать никаких действий для самостоятельного или с привлечением сторонних ИТ-специалистов поиска и удаления компьютерных вирусов, восстановления работоспособности ЭУ, не отправлять ЭУ в сервисные службы ИТ для восстановления работоспособности.
11. Зафиксировать в протокольной форме значимые действия и события, в т.ч. имена лиц, имеющих доступ к ЭУ, действия с ЭУ, подключенным к Системе ДБО, предшествовавшие факту хищения денежных средств, подготовить объяснения работников об использовании ЭУ в целях, отличных от осуществления операций в Системе ДБО, посещаемых сайтах, о странностях при работе ЭУ, перебоях или отказах ЭУ, обращениях в ИТ-службы, в банк, о сторонних лицах, побывавших в месте расположения ЭУ и т.д.
12. Все действия, указанные в пунктах 1, 5, 8, 9, 11 настоящих Рекомендаций, производить коллегиально, протоколировать и документировать, в т.ч. с использованием фотосъемки. При невозможности осуществления коллегиальных действий (для индивидуальных предпринимателей или физических лиц, занимающихся частной практикой) отдельно зафиксировать данный факт.
13. Оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств.
14. Оперативно обратиться в суд с исковым заявлением о взыскании денежных средств с получателя денежных средств (указав все известные реквизиты получателя), а также с ходатайством о принятии судом мер по обеспечению иска в виде ареста денежных средств на счете получателя.

Банк вправе по своему усмотрению в одностороннем порядке вносить изменения в данные Рекомендации с уведомлением Клиента об этом путем размещения соответствующей информации на официальном сайте банка.

Республиканский Кредитный Альянс

Коммерческий Банк

Приложение № 1

ПРИМЕРНЫЙ ОБРАЗЕЦ ЗАЯВЛЕНИЯ
В БАНК ОБ ОТЗЫВЕ ПЛАТЕЖА, ВОЗВРАТЕ ДЕНЕЖНЫХ СРЕДСТВ И БЛОКИРОВАНИИ ДОСТУПА К СИСТЕМЕ ДБО

_____
должность руководителя банка
_____
наименование банка
_____
ФИО
_____
(наименование организации/ИП)
_____
(должность и ФИО руководителя)

"__" _____ 202_ года с нашего банковского счета, открытого в Вашем банке, по Системе дистанционного банковского обслуживания были похищены денежные средства, которые, по имеющейся информации были переведены со следующими реквизитами платежа:

Дата платежа: _____
Номер распоряжения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____

Наименование банка получателя: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____

Прошу Вас заблокировать доступ к системе ДБО, провести процедуру компрометации всех Секретных ключей и оказать содействие в возврате денежных средств.

_____ _____ _____
должность подпись расшифровка подписи

"__" _____ 202__

тел. _____

Республиканский Кредитный Альянс

Коммерческий Банк

Приложение № 2

ПРИМЕРНЫЙ ОБРАЗЕЦ ЗАЯВЛЕНИЯ
В БАНК ПОЛУЧАТЕЛЯ ИЛИ К ОПЕРАТОРУ ПЛАТЕЖНОЙ СИСТЕМЫ О ПРИОСТАНОВЛЕНИИ ПЛАТЕЖА И ВОЗВРАТЕ ДЕНЕЖНЫХ СРЕДСТВ

_____
должность руководителя банка
_____
наименование банка
_____
ФИО
_____
(наименование организации/ИП)
_____
(должность и ФИО руководителя)

"__" _____ 202__ года с нашего банковского счета были похищены денежные средства, которые, по информации, полученной из банка, были переведены со следующим реквизитам платежа:

Дата платежа: __
Номер распоряжения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____

Наименование банка получателя: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____

Прошу Вас оказать содействие в приостановлении прохождения платежа и возврате денежных средств.

_____ _____ _____
должность подпись расшифровка подписи

"__" _____ 202__

тел. __

Приложение № 3

ПРИМЕРНЫЙ ОБРАЗЕЦ ПИСЬМА
ИНТЕРНЕТ ПРОВАЙДЕРУ О ПРЕДОСТАВЛЕНИИ ЖУРНАЛОВ СОЕДИНЕНИЙ (ЛОГОВ)

_____
(должность руководителя)
_____
(наименование организации)
_____
ФИО

от _____
должность, ФИО заявителя
проживающего: _____
адрес места жительства
паспорт: _____
номер паспорта, дата выдачи,
кем и когда выдан
контактный телефон: _____
телефон заявителя
адрес для корреспонденции _____
почтовый адрес

"__" _____ 20__ года в __:__ по московскому времени со счета _____ по Системе дистанционного банковского обслуживания (ДБО) был осуществлен несанкционированный перевод денежных средств.
Компьютер, с которого осуществляется подключение к Системе ДБО, располагается по адресу _____ и использует IP-адрес ___.___.___.___.
Вероятной причиной несанкционированного перевода могло послужить заражение компьютера вредоносным программным обеспечением, кража логина, пароля и Секретных ключей Системы ДБО.
"__" _____ 20__ года между _____ и вами был заключен договор N _____ об оказании _____ услуг.
Для выявления обстоятельств несанкционированного перевода прошу предоставить информацию из журналов (логов) о входящем и исходящем трафике за период с "__" _____ 20__ года по "__" _____20__ года с указанием времени соединения, IP и MAC адресов.

_____ _____ _____
должность подпись расшифровка подписи

"__" _____ 20__